

一种密文混合运算方法及装置

5 本申请要求于 2022 年 03 月 15 日提交中国专利局、申请号为 202210252212.3、申请名称为“一种密文混合运算方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本说明书涉及密文运算领域，尤其涉及一种密文混合运算方法及装置。

背景技术

10 现代计算机系统常常需要使用不同数据类型处理不同种类的信息，当面对使用不同类型数据的某一运算时，可以使用混合运算的方式以得到符合该某一运算要求的运算结果。
在相关技术中，针对明文数据的混合运算已存在一系列成熟的解决方案，但对于密文数据的混合运算的研究仍然处于初期阶段，没有形成任何统一、高效且清晰的方案。

发明内容

15 有鉴于此，本说明书提供一种密文混合运算方法及装置，以解决相关技术中存在的不足。

具体地，本说明书是通过如下技术方案实现的：

20 根据本说明书实施例的第一方面，提供了一种服务告警方法，用于对多种预设密文类型的密文进行混合运算，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，并基于所述单向密文转换关系形成多层级密文转换关系，每一预设密文类型在所述多层级密文转换关系中对应有唯一的层级，且每一预设密文类型与最高层级的预设密文类型之间至少存在一条由所述单向密文转换关系构成的路径，所述方法包括：

25 接收目标函数签名以及对应的操作数集合，所述操作数集合包含对应于至少两种预设密文类型的密文操作数；

确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中；

在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标

函数签名所指定的运算函数对转换后的密文操作数进行运算。

根据本说明书实施例的第二方面，提供了一种服务告警装置，用于对多种预设密文类型的密文进行混合运算，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，并基于所述单向密文转换关系形成多层级密文转换关系，每一预设密文类型在所述多层级密文转换关系中对应有唯一的层级，且每一预设密文类型与最高层级的预设密文类型之间至少存在一条由所述单向密文转换关系构成的路径，所述装置包括：

数据接收单元，用于接收目标函数签名以及对应的操作数集合，所述操作数集合包含对应于至少两种预设密文类型的密文操作数；

目标密文类型确定单元，用于确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中；

数据运算单元，用于在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

根据本说明书实施例的第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现如第一方面所述的方法的步骤。

根据本说明书实施例的第四方面，提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如第一方面所述的方法的步骤。

在本说明书所提供的技术方案中，通过引入基于多层级密文转换关系，有效管理了多种预设密文类型之间的转换关系，使得在使用不同类型数据的密文进行某一运算时，可以根据该多层级密文转换关系清晰、高效地确定各密文的转换关系以得到符合上述某一运算要求的最终结果。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书。

附图说明

图 1 是本说明书一示例性实施例示出的一种多层级密文转换关系的结构示意图；
图 2 是本说明书一示例性实施例示出的一种密文混合运算方法的流程示意图；
图 3 是本说明书一示例性实施例示出的一种优化的密文混合运算方法的示意图；
图 4 是本说明书一示例性实施例示出的一种电子设备的示意结构图；
图 5 是本说明书一示例性实施例示出的一种密文混合运算装置的结构示意图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

在相关技术中，存在有诸如数据库系统等支持弱类型的混合运算的应用或系统，使得用户在使用过程中无需关注各种类型的数据在任一混合运算时有关类型转换的操作，但这也导致用户无法直观的判断上述应用或系统是否支持该任一混合运算。事实上，以上问题可以通过使用类型系统解决，类型系统为防止程序在运行混合运算等过程时发生类型错误的系统。根据参与混合运算的数据的可读性、安全性可以将类型系统划分为针对明文数据的明文数据类型系统以及针对密文数据的密文数据类型系统。

对于明文数据而言，相关技术中已存在着一系列成熟且支持基于类型转换、函数重载、默认规则的混合运算方案的明文数据类型系统可以较为容易地解决上述问题。

但对于密文数据而言，由于存在有以下问题导致有关密文数据类型系统的研究程度较低，进而难以像明文数据类型系统一样可以较为容易地解决上述问题：1) 未发现合适的逻辑结构以应用于不同类型密文间的混合运算；2) 用户无法清晰地获知不同类型密文间的混合运算结果的类型，进而无法验证结果正确性 3) 类比针对明文类型的混合运算方案，完整支持密文类型的混合运算方案涉及修改已有系统核心逻辑，实现不同密文类型的分类与默认规则，开发量大且难以维护；4) 密文类型转换相关技术中需要使用 TEE 可信执行环境 (Trusted Execution Environment, TEE) 进行密文类型转换，资源开销较大；5) 相关技术中不支持明密文混合计算，应用场景较小。

此外，无论是对于明文数据，或是密文数据，相关技术中确定其混合运算结果的类型时都需要经过繁杂的匹配操作。例如：一类型系统中存在函数签名分别匹配 `int8+float4`、`int8+int8`、`float4+float4`、`decimal+decimal`、`int8=float4` 的函数，又存在目标函数“`a+b`”，其中，操作数“`a`”的类型为 `int8`，操作数“`b`”的类型为 `text`。显然，该类型系统中不存在严格匹配“`int8+text`”的函数签名，上述类型系统首先需要查询所有支持“`+`”的函数签

名 (即 `int8+float4`、`int8+int8`、`float4+float4`、`decimal+decimal`)，并从中确定出操作数类型与目标函数中的操作数部分匹配的函数签名 (即 `int8+float4`、`int8+int8`)，然后根据上述类型系统对应的预设规则判断操作数 `b` 是否可以转换为“float4”或者“int8”，若转换失败，则确定所有支持“+”的函数签名中操作数类型与目标函数完全不匹配的函数签名 (即 `float4+float4`、`decimal+decimal`)，并根据上述预设规则判断目标函数中的“int8”和“text”能否分别转化为 float4 或 decimal，若上述预设规则设置 int8 可以转换为 float4 或 decimal，text 无法转换为 float4 但可以转换为 decimal，则上述类型系统可以确定将 int8 和 text 一同转换为 decimal 类型并执行“+”运算。

为解决上述相关技术中的问题，本说明书提供一种密文混合运算方案，该方案基于诸如图 1 所示的多层级密文转换关系实现。图 1 是本说明一示例性实施例的一种多层级密文转换关系的结构示意图。如图 1 所示，该多层级密文转换关系可以用于对多种预设密文类型的密文进行混合运算。其中，上述多种预设密文类型中存在有原始密文类型与对应的目的密文类型，二者之间通过连线的方式设置有由原始密文类型指向目的密文类型的单向密文转换关系，该单向密文转换关系定义了上述原始密文类型可以转换为上述目的密文类型，但上述目的密文类型却无法转换为上述原始密文类型。每一预设密文类型在上述多层级密文转换关系中对应有唯一的层级，因此多层级密文转换关系可由一条或多条各预设密文类型之间的单向密文转换关系形成。此外每一预设密文类型与最高层级的预设密文类型之间至少存在一条由上述单向密文转换关系构成的路径，确保了两个预设密文类型至少可以转换为最高层级的预设密文类型进行函数运算。

例如，如图 1 所示，该多层级密文转换关系由 7 种预设密文类型组成，其中，“enc_text”与“enc_int4”属于同一种预设密文类型的不同对象，“enc_base”为预设密文类型外的字面量类型，该字面量类型可以用于表述没有携带类型信息的密文数据。根据预设密文类型的属性可以将上述多个预设密文类型分别划分至诸如“字符密文类型”、“字符串密文类型”与“时间密文类型”等不同属性。其中，每一预设密文类型支持有对应的操作函数，且每一属性下的预设密文类型支持有类似的操作函数，例如数值密文类型“enc_int4”、“enc_int8”支持“=，>，+，/”四种操作函数，字符串密文类型“enc_text”支持“=，>，||”三种操作函数。同时在该多层级密文转换关系中针对上述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系。例如根据层级可以将“enc_int4”与“enc_int8”的连线表征为一条由“enc_int4”指向“enc_int8”的单向密文转换关系，本领域技术人员容易想到的是，当存在两个密文类型分别为“enc_int4”、“enc_int8”的操作数进行“=”函数运算时，用户可以根据上述“enc_int4”与“enc_int8”之间的密文转换关系以及“enc_int8”所支持的操作函数可以容易地推断出密文类型为“enc_int4”的操作数转化为“enc_int8”后与另一个密文类型同为“enc_int8”的操作数可以实现“=”函数运算，但在相关技术中由于不存在包含有关密文的转换关系，导致用户难以预测运算结果的密文类型。基于上述单向密文转换关系可形成有多层级密文转换关系，其中每一预设密文类型

与最高层级的预设密文类型“enc_text”之间至少存在一条由上述单向密文转换关系构成的路径,例如“enc_float4”与“enc_text”之间存在“enc_float4”-“enc_float8”-“enc_decimal”-“enc_text”这一路径,或者“enc_text”与“enc_text”之间存在“enc_text”-“enc_decimal”-“enc_text”与“enc_text”-“enc_timestamp”-“enc_text”这两条路径。

5 对于数据库系统等支持部分运算函数下不同属性的预设密文类型之间的双向转换的系统,上述多层级密文转换关系中针对上述双向转换过程中的任一方预设密文类型设置虚拟密文类型。其中,上述虚拟密文类型与上述一方预设密文类型的密文类型相同。

在一实施例中,上述多层级密文转换关系中在第一预设密文类型与第二预设密文类型,在二者之间相互存在上述单向密文转换关系的情况下,上述多种预设密文类型中包含与上述第一预设密文类型具有相同密文类型的虚拟密文类型,且由上述第二预设密文类型指向上述第一预设密文类型的单向密文转换关系被替换为由上述第二预设密文类型指向上述虚拟密文类型。该实施例的方案使得上述多层级密文转换关系中规避了由于存在两个预设密文类型之间相互存在上述单向密文转换关系导致的环结构。以图1中的多层级密文转换关系为例,由于预设密文类型“enc_decimal”与“enc_text”在数据库等系统中相互存在上述单向密文转换关系,导致其他预设密文类型无法确定上述最高层级的预设密文类型为“enc_decimal”或是“enc_text”,故所述多层级密文转换关系中创建虚拟密文类型“enc_text”并创建由预设密文类型“enc_decimal”指向预设密文类型“enc_text”的单向密文转换关系,进而避免了由预设密文类型“enc_decimal”指向预设密文类型“enc_text”的单向密文转换关系。

20 本领域技术人员可以理解的是,上述多层级密文转换关系中各预设密文类型的层级可以根据实际情况确定,例如根据相关技术中明文数据类型系统中已存在的明文类型的转换规则,或本领域中约定俗成的规则,或代表性的行业规范,以诸如各预设密文类型的数据精度大小等信息确定各预设密文类型的层级。又例如根据用户预先定义的其他规则以确定各预设密文类型的层级。本说明书中并不对此进行限制。

25 下面结合图2所示实施例对本说明书的技术方案进行阐述。图2是本说明书一示例性实施例示出的一种密文混合运算方法的流程示意图,如图2所示,该方法可以包括以下步骤:

S201,接收目标函数签名以及对应的操作数集合,所述操作数集合包含对应于至少两种预设密文类型的密文操作数。

30 上述目标函数签名为对应运算函数的描述信息,该描述信息中包括但不限于上述对应运算函数的参数数量以及各参数的类型、返回值类型。换言之,上述目标函数签名指向对应运算函数且可以用于定义该对应运算函数的输出与输入情况。上述操作数集合中各操作数分别对应上述目标函数签名所指定的运算函数的参数。

在上述密文混合运算的过程中,上述操作数集合应当包含对应于至少两种预设密文类型的密文操作数。当然,当操作数集合中所有密文操作数所对应的预设密文类型种类小于

两个时，可判断该操作数集合中是否存在明文操作数，若存在，则可以将明文操作数包装为对应密文类型的密文操作数，使得上述多层级密文转换关系可以兼容于明文混合运算或者明文与密文混合运算；若不存在，则意味着该操作数集合中仅存在对应同一种预设密文类型的密文操作数，则可以直接将上述同一种预设密文类型确定为目标密文类型进行后续运算。

其中，当上述操作数集合存在有不属于任一预设密文类型的未知密文类型时，可以向用户提示相应的错误信息，或者根据用户预先定义的转换规则将该未知密文类型强制转换为指定预设密文类型，本说明书中并不对此进行限制。

S202，确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中。

上述目标密文类型为上述至少两种预设密文类型在运算过程中共同转换的密文类型。事实上，只有统一上述至少两种预设密文类型的类型才能够满足对应运算函数进行运算操作的前提条件。

由于无法确定上述至少两种预设密文类型分别与上述最高层级的预设密文类型之间形成的路径中重叠部分的路径长度，且目标密文类型来源于上述路径中的预设密文类型，所以可以确定在基于多层级密文转换关系的密文混合运算中可能存在有同时确定一种或多种目标密文类型的情况。

在一实施例中，当存在多种预设密文类型同时处于上述至少两种预设密文类型分别与上述最高层级的预设密文类型之间形成的路径中时，上述目标密文类型为其中层级最低的预设密文类型。上述层级最低的预设密文类型保证了选择的目标密文类型过程中的唯一性，同时由于上述路径中多种预设密文类型的确定顺序是由上述至少两种预设密文类型所处的低层级自下而上向上述最高层级的预设密文类型进行的，故选择上述路径中层级最低的预设密文类型为目标密文类型可以节省对于额外预设密文类型的确定操作，有效提高了目标密文类型。此外在前文所述以数据精度大小确定各预设密文类型的层级的情况下，选择上述路径中层级最低的预设密文类型为目标密文类型可以保证目标密文类型的精度大小最优化，从而提高了数据空间管理效率。

对于上述多种预设密文类型可以引入特定的集合类型实现，以满足实际情况下对于确定所述至少两种预设密文类型对应的目标密文类型的性能要求。上述特定的集合类型可以为“图”或“格(lattice)”等结构，其中，“格”为一种偏序集合，其任意非空有限子集都有一个上确界和一个下确界，当上述多种预设密文类型通过“格”结构实现时，该多种预设密文类型可属于基于格的偏序集中的元素。

在一实施例中，确定上述操作数集合中的密文操作数对应的上述至少两种预设密文类型在上述偏序集中对应的上确界，即可作为上述目标密文类型。其中，该上确界对应相当于同时处于上述至少两种预设密文类型分别与上述最高层级的预设密文类型之间形成的路径中的所有预设密文类型，故通过确定“格”结构中的上确界可以更加高效、直观地确

定上述目标密文类型。同时，本领域技术人员可以理解的是，例如前文所述选择上述路径中层级最低的预设密文类型为目标密文类型的方式等效于本实施例中选择最小上确界。

上述偏序集可以基于拓扑序列确定上述目标密文类型。其中，拓扑序列中各元素的边可以对应于上述单向密文转换关系，且每一单向密文转换关系中的原始密文类型在上述拓扑序列中对应的序号小于对应的目的密文类型在所述拓扑序列中对应的序号。

在一实施例中，比较上述至少两种预设密文类型中N种预设密文类型在上述拓扑序列中对应的序号大小，当上述N种预设密文类型对应的序号不完全一致时，将上述N种预设密文类型中对应非最大序号的预设密文类型分别更新为与之在上述拓扑序列中的边所对应的预设密文类型，直至上述N种预设密文类型对应的序号一致，上述N为上述至少两种预设密文类型中预设密文类型的种类数目；将上述拓扑序列中与上述N种预设密文类型的序号对应的预设密文类型确定为目标密文类型。由于拓扑序列结构简单、维护方便等优点，使得在实际应用场景中构建多层级密文转换关系时针对用户的技术门槛减低，技术可行性增加。

以基于拓扑序列确定目标密文类型为例，结合图3对本说明书中涉及上述实施例的技术方案进行详细阐述。图3是一示例性实施例示出的一种优化的密文混合运算方法的示意图，如图3所示，该拓扑序列中的元素与边根据图1的多层级密文转换关系。其中，拓扑序列中各元素的边可以对应于上述多层级密文转换关系中各单向密文转换关系。当存在两个分别对应预设密文类型“enc_timestamp”与“enc_int8”操作数时，显然，在上述拓扑序列中，两个操作数对应的预设密文类型的序号分别为“2”与“4”，则根据上述拓扑序列中与元素“enc_timestamp”对应的边可以将对应预设密文类型序号较小（即对应序号2的预设密文类型“enc_timestamp”）的操作数由预设密文类型“enc_timestamp”转换为采用“enc_text”进行表征。此时两个操作数对应预设密文类型的序号分别为“8”与“4”；由于上述序号并不一致，故根据上述拓扑序列中与元素“enc_int8”对应的边可以将对应预设密文类型序号较小（即对应序号4的预设密文类型“enc_int8”）的操作数由预设密文类型“enc_int8”转换为采用“enc_float8”进行表征。此时两个操作数对应预设密文类型的序号分别为“8”与“6”；由于上述序号依然不一致，所以继续根据上述拓扑序列中与元素“enc_float8”对应的边可以将对应预设密文类型序号较小（即对应序号6的预设密文类型“enc_float8”）的操作数由预设密文类型“float8”转换为采用“enc_decimal”进行表征。此时两个操作数对应预设密文类型的序号分别为“8”与“7”；由于上述序号还是不一致，所以继续根据上述拓扑序列中与元素“enc_decimal”对应的边可以将对应预设密文类型序号较小（即对应序号7的预设密文类型“enc_decimal”）的操作数由预设密文类型“decimal”转换为采用“enc_text”进行表征。此时两个操作数对应预设密文类型的序号均为“8”即两个操作数对应预设密文类型的序号相同，可以将上述拓扑序列中与序号“8”对应的预设密文类型“enc_text”确定为目标密文类型。

由于字面量类型未携带类型信息，故而在类似于数据库等系统下的字面量类型与任一

密文类型进行运算时，类型系统可以优先尝试将该字面量类型直接转换为采用上述任一密文类型进行表征，若转换失败，则该类型系统可以向用户提示相应的错误信息。总之，上述拓扑序列中不需要特意地设置有关字面量类型“enc_base”的元素。

由于多层级密文转换关系中可能存在有多条由同一原始密文类型指向不同目的密文类型的单向密文转换关系，故可以在上述拓扑序列中设置上述虚拟密文类型，以建立由该原始密文类型指向该虚拟密文类型的单向密文转换关系以及由该虚拟密文类型的指向上述不同目的密文类型的单向密文转换关系。其中该虚拟密文类型可以用于比较虚拟密文类型与上述不同目的密文类型中每一目的密文类型在拓扑序列的序号大小，若相同则将该原始密文类型转化为采用该每一目的密文类型进行表征，否则继续尝试比较该虚拟密文类型与上述不同目的密文类型中其他目的密文类型在拓扑序列的序号大小。该虚拟密文类型的应用减少了确定上述多条由同一原始密文类型指向不同目的密文类型的单向密文转换关系其中一条单向密文转换关系的判断复杂度，进而提高了基于该多层级密文转换关系的混合运算效率。

以图3中的拓扑序列为例：由于预设密文类型“enc_text”分别与预设密文类型“enc_timestamp”、“enc_decimal”存在单向密文转换关系，故可以在该拓扑序列设置序号为“2”的虚拟密文类型“enc_timestamp'”。当两个分别对应预设密文类型“enc_text”、“enc_timestamp”的操作数进行函数运算时，可以将对应预设密文类型“enc_text”的转换操作数为采用预设密文类型“enc_timestamp'”进行表征后，判断两个操作数对应的预设密文类型的序号大小，由于预设密文类型“enc_timestamp'”与“enc_timestamp”实际上属于同一密文类型，故预设密文类型“enc_timestamp'”与“enc_timestamp”的序号“1”、“2”可视为同一序号，使得可以将对应预设密文类型“enc_timestamp'”的操作数转换为采用预设密文类型“enc_timestamp”进行表征。或者，当两个分别对应预设密文类型“enc_text”、“enc_int8”的操作数进行函数运算时，将对应预设密文类型“enc_text”的操作数转换为采用预设密文类型“enc_timestamp'”进行表征后，判断两个操作数对应的预设密文类型的序号大小，显然，预设密文类型“enc_int8”与“enc_timestamp'”对应的序号是不相等，则将对对应预设密文类型“enc_timestamp'”的操作数转换为采用预设密文类型“enc_text”进行表征后，继续与对应预设密文类型“enc_int8”的操作数比较对应的预设密文类型的序号大小，并重复以上操作直到两个操作数的密文类型在该拓扑序列中对应的序号大小相同。

S203，在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

由于不同的密文类型支持有不同的运算函数，故在基于多层级密文转换关系中密文混合运算中可以根据上述目标密文类型对于上述目标函数签名所指定的运算函数的支持情况做出相应操作。

当确定上述目标密文类型支持上述目标函数签名所指定的运算函数时，可以将操作数集合中所有密文操作数解密为明文操作数后再转换为采用上述目标密文类型进行表征，并根据上述目标函数签名中的运算函数得到最终的运算结果。例如：存在一目标函数签名 A 仅包含两个操作数，且指定的运算函数为“+”，当两个操作数的密文类型分别为“enc_int4”与“enc_text”，且分别对应明文“12”与“3”，以及目标密文类型为“enc_decimal”时，5 可以将上述两个操作数的密文类型共同转换为采用“enc_decimal”表征并运算得到最终的运算结果“15”。同时，本领域技术人员可以理解的是：上述“所有密文操作数”可以为操作数集合中所有的操作数，例如上述操作数集合中仅存在不同密文类型的操作数 a、b、c，上述运算函数为“a+b+c”且目标密文类型支持“+”函数时，可将 a、b、c 解密并转换为采用上述目标密文类型进行表征；或者，上述“所有密文操作数”可以为操作数集合中对应上述运算函数中的部分运算函数的操作数，例如上述操作数集合中存在不同密文类型的操作数 a、b、c，且上述的运算函数为“(a+b)||c”，如果多层级密文转换关系中不存在同时支持“+”与“||”的预设密文类型，则可将上述运算函数“(a+b)||c”作为父运算函数并拆分为两个子运算函数，每个子运算函数仅包含该父运算函数的部分运算函数，其中：10 可以先将子运算函数“(a+b)”作为一独立的运算函数，确定该子运算函数所涉及的操作数 a 和 b 对应的目标密文类型，再将该子运算函数“(a+b)”的运算结果作为新的操作数 d，参与另一子运算函数“d||c”的函数运算，并将该子运算函数“d||c”作为一独立的运算函数，确定该子运算函数所涉及的操作数 d 和 c 对应的目标密文类型。可见，对于较为复杂的运算函数，本说明书可以将该运算函数作为父运算函数进行拆分，并对拆分形成的每一子运算函数分别确定一次目标密文类型，即可将每一子运算函数的函数运算过程视作一次独立的混合运算，并最终得到父运算函数的混合运算结果。其中，如果一子运算函数不依赖于其他的子运算函数，譬如上述的子运算函数“(a+b)”，则该子运算函数所涉及的操作数均来自父运算函数对应的操作数集合；如果一子运算函数依赖于其他的子运算函数，譬如上述的子运算函数“d||c”，则该子运算函数所涉及的操作数可能部分来自父运算函数对应的操作数集合（比如操作数 c），且必然存在至少一部分操作数为其依赖的其他子运算函数的运算结果（比如操作数 d），甚至其涉及的所有操作数都有可能来自其依赖的其他子运算函数的运算结果。25

当确定上述目标密文类型不支持上述目标函数签名所指定的运算函数时，可以在上述目标密文类型与上述最高层级的预设密文类型之间形成的路径中，选取其他预设密文类型以更新上述目标密文类型，上述其他预设密文类型支持上述目标函数签名对应的函数。上述目标密文类型的更新操作包含有“循环遍历”的设计思想，即通过重复尝试判断上述其他预设密文类型是否支持上述目标函数签名对应的函数已确定最终的目标密文类型，其中，上述其他预设密文类型的选择顺序可以根据层级大小等规则设置，本说明书中并不对此进行限制。在上述目标密文类型不支持上述目标函数签名对应的函数，且不存在其他预设密文类型的层级大于上述目标密文类型的层级的情况下，可以向用户提示相应的错误信息。30 35

当上述操作数集合中包含字面量类型的操作数时，可以保证该字面量类型的操作数依然能够参与上述运算函数的运算。

在一实施例中，将上述对应于至少两种预设密文类型的密文操作数以及对应于字面量类型的密文操作数解密后分别转换为采用上述目标密文类型进行表征，并根据上述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。例如前文所述，字面量类型可以用于表述没有携带类型信息的密文数据，故可以尝试将上述对应于字面量类型的密文操作数与上述对应于至少两种预设密文类型的密文操作数一同解密并分别转换为目标密文类型的操作数参与后续运算过程。

上述多种预设密文类型所含的预设密文类型以及上述多层级密文转换关系中的任一单向密文转换关系可以根据实际需求修改。

在一实施例中，上述多层级密文转换关系可以根据接收到的调整指令，调整上述多种预设密文类型所含的预设密文类型和/或所述多层级密文转换关系中的任一单向密文转换关系。其中，调整指令可以包含某一预设密文类型的名称、支持的运算函数以及与上述多层级密文转换关系中某一单向密文转换关系的特征信息，根据该调整指令可以将上述某一预设密文类型和/或上述某一单向密文转换关系新增至上述多层级密文转换关系中；或者删除、修改上述多层级密文转换关系中对应上述某一预设密文类型和/或上述某一单向密文转换关系的数据。

本领域技术人员可以理解的是，本说明书的方案可以基于 TEE 将操作数集合中所有密文操作数解密后转换为采用目标密文类型进行表征，并根据目标函数签名所指定的运算函数对转换后的密文操作数进行运算。其中，相较于相关技术中，由于密文运算规则的规定需要执行至少两次 TEE 操作（即第一次 TEE 操作：将密文操作数在 TEE 中解密得到明文操作数，并将明文操作数转换至对应目标密文类型后，加密明文操作数为密文操作数；第二次 TEE 操作，将加密后的密文操作数再次解密为明文操作数，根据目标函数对明文操作数进行运算，将运算结果加密输出），本说明书的方案可以执行一次 TEE 操作（即将密文操作数在 TEE 中解密得到明文操作数，将明文操作数转换至对应目标密文类型后，根据目标函数对明文操作数进行运算，最后将运算结果加密输出）即可完成密文混合运算，进而减低了使用 TTE 造成的系统开销，提高了执行 TEE 操作的效率。

通过上述实施例可知，本说明书中密文混合运算方法，通过引入基于格的多层级密文转换关系，有效管理了多种预设密文类型之间的转换关系，使得用户在使用不同类型数据的密文进行某一运算时，可以根据该多层级密文转换关系清晰、高效地确定各密文的转换关系以得到符合上述某一运算要求的最终结果。同时上述多层级密文转换关系可以作为独立子系统嵌入已涉及密文计算的产品，且该过程不涉及更改已有系统核心逻辑，使得上述多层级密文转换关系易于进行新增类型、函数等操作。此外多层级密文转换关系在实现完整匹配功能的同时，还可以实现了相比传统密文运算方法更低的系统开销。又由于可以通过将明文包装成对应的密文类型的方式，使得上述密文数据类型系统支持明密文混合计

算，提高了本说明书中本多层级密文转换关系的应用场景。

图 4 是一示例性实施例中的一种电子设备的示意结构图。请参考图 4，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他功能所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成密文混合运算装置。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

与前述密文混合运算方法的实施例相对应，本说明书还提供了密文混合运算装置的实施例。

10 请参考图 5，图 5 是一示例性实施例示出的一种密文混合运算装置的结构示意。如图 5 所示，在软件实施方式中，该密文混合运算装置用于对多种预设密文类型的密文进行混合运算，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，并基于所述单向密文转换关系形成多层级密文转换关系，每一预设密文类型在所述多层级密文转换关系中对应有唯一的层级，且每一预设密文类型与最高层级的预设密文类型之间至少存在一条由所述单向密文转换关系构成的路径，该密文混合运算装置可以包括：

数据接收单元 501，用于接收目标函数签名以及对应的操作数集合，所述操作数集合包含对应于至少两种预设密文类型的密文操作数。

20 目标密文类型确定单元 502，用于确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中。

数据运算单元 503，用于在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

25 可选的，所述装置还包括：

目标密文类型选择单元 504，用于当存在多种预设密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中时，所述目标密文类型为其中层级最低的预设密文类型。

30 可选的，所述数据运算单元 503 具体用于：将所述对应于至少两种预设密文类型的密文操作数以及对应于字面量类型的密文操作数解密后分别转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

可选的，所述多种预设密文类型属于基于格的偏序集中的元素，所述目标密文类型确定单元 502 具体用于：

35 确定所述操作数集合中的密文操作数对应的所述至少两种预设密文类型在所述偏序集中对应的上确界，以作为所述目标密文类型。

可选的，所述偏序集基于拓扑序列进行表征，所述拓扑序列中各元素的边对应于所述单向密文转换关系，且每一单向密文转换关系中的原始密文类型在所述拓扑序列中对应的序号小于对应的目的密文类型在所述拓扑序列中对应的序号，所述目标密文类型确定单元502具体用于：

- 5 比较所述至少两种预设密文类型中N种预设密文类型在所述拓扑序列中对应的序号大小，当所述N种预设密文类型对应的序号不完全一致时，将所述N种预设密文类型中对应非最大序号的预设密文类型分别更新为与之在所述拓扑序列中的边所对应的预设密文类型，直至所述N种预设密文类型对应的序号一致，所述N为所述至少两种预设密文类型中预设密文类型的种类数目；
- 10 将所述拓扑序列中与所述N种预设密文类型的序号对应的预设密文类型确定为目标密文类型。

可选的，所述装置具体用于：

- 15 在第一预设密文类型与第二预设密文类型之间相互存在所述单向密文转换关系的情况下，所述多种预设密文类型中包含与所述第一预设密文类型具有相同密文类型的虚拟密文类型，且由所述第二预设密文类型指向所述第一预设密文类型的单向密文转换关系被替换为由所述第二预设密文类型指向所述虚拟密文类型。

可选的，所述装置还包括：

- 20 目标密文类型更新单元505，用于在所述目标密文类型不支持所述目标函数签名对应的函数的情况下，在所述目标密文类型与所述最高层级的预设密文类型之间形成的路径中选取其他预设密文类型以更新所述目标密文类型，所述其他预设密文类型支持所述目标函数签名对应的函数。

多层级密文转换关系调整单元506，用于根据接收到的调整指令，调整所述多种预设密文类型所含的预设密文类型和/或所述多层级密文转换关系中的任一单向密文转换关系。

- 25 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

- 30 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

- 35 本说明书中描述的主题及功能操作的实施例可以在以下中实现：数字电子电路、有形体现的计算机软件或固件、包括本说明书中公开的结构及其结构性等同物的计算机硬件、或者它们中的一个或多个的组合。本说明书中描述的主题的实施例可以实现为一个或多个计算机程序，即编码在有形非暂时性程序载体上以被数据处理装置执行或控制数据处理装

置的操作的计算机程序指令中的一个或多个模块。可替代地或附加地，程序指令可以被编码在人工生成的传播信号上，例如机器生成的电、光或电磁信号，该信号被生成以将信息编码并传输到合适的接收机装置以由数据处理装置执行。计算机存储介质可以是机器可读存储设备、机器可读存储基板、随机或串行存取存储器设备、或它们中的一个或多个的组合。

本说明书中描述的处理及逻辑流程可以由执行一个或多个计算机程序的一个或多个可编程计算机执行，以通过根据输入数据进行操作并生成输出来执行相应的功能。所述处理及逻辑流程还可以由专用逻辑电路—例如 FPGA（现场可编程门阵列）或 ASIC（专用集成电路）来执行，并且装置也可以实现为专用逻辑电路。

适合用于执行计算机程序的计算机包括，例如通用和/或专用微处理器，或任何其他类型的中央处理单元。通常，中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的基本组件包括用于实施或执行指令的中央处理单元以及用于存储指令和数据的一个或多个存储器设备。通常，计算机还将包括用于存储数据的一个或多个大容量存储设备，例如磁盘、磁光盘或光盘等，或者计算机将可操作地与此大容量存储设备耦接以从其接收数据或向其传送数据，抑或两种情况兼而有之。然而，计算机不是必须具有这样的设备。此外，计算机可以嵌入在另一设备中，例如移动电话、个人数字助理（PDA）、移动音频或视频播放器、游戏操纵台、全球定位系统（GPS）接收机、或例如通用串行总线（USB）闪存驱动器的便携式存储设备，仅举几例。

适合于存储计算机程序指令和数据的计算机可读介质包括所有形式的非易失性存储器、媒介和存储器设备，例如包括半导体存储器设备（例如 EPROM、EEPROM 和闪存设备）、磁盘（例如内部硬盘或可移动盘）、磁光盘以及 CD ROM 和 DVD-ROM 盘。处理器和存储器可由专用逻辑电路补充或并入专用逻辑电路中。

虽然本说明书包含许多具体实施细节，但是这些不应被解释为限制任何发明的范围或所要求保护的发明，而是主要用于描述特定发明的具体实施例的特征。本说明书内在多个实施例中描述的某些特征也可以在单个实施例中被组合实施。另一方面，在单个实施例中描述的各种特征也可以在多个实施例中分开实施或以任何合适的子组合来实施。此外，虽然特征可以如上所述在某些组合中起作用并且甚至最初如此要求保护，但是来自所要求保护的组合中的一个或多个特征在一些情况下可以从该组合中去除，并且所要求保护的组合可以指向子组合或子组合的变型。

类似地，虽然在附图中以特定顺序描绘了操作，但是这不应被理解为要求这些操作以所示的特定顺序执行或顺次执行、或者要求所有例示的操作被执行，以实现期望的结果。在某些情况下，多任务和并行处理可能是有利的。此外，上述实施例中的各种系统模块和组件的分离不应被理解为在所有实施例中均需要这样的分离，并且应当理解，所描述的程序组件和系统通常可以一起集成在单个软件产品中，或者封装成多个软件产品。

由此，主题的特定实施例已被描述。其他实施例在所附权利要求书的范围以内。在某

些情况下，权利要求书中记载的动作可以以不同的顺序执行并且仍实现期望的结果。此外，附图中描绘的处理并非必需所示的特定顺序或顺次顺序，以实现期望的结果。在某些实现中，多任务和并行处理可能是有利的。

- 5 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

权 利 要 求 书

1、一种密文混合运算方法，其特征在于，用于对多种预设密文类型的密文进行混合运算，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，并基于所述单向密文转换关系形成多层级密文转换关系，每一预设密文类型在所述
5 多层级密文转换关系中对应有唯一的层级，且每一预设密文类型与最高层级的预设密文类型之间至少存在一条由所述单向密文转换关系构成的路径，所述方法包括：

接收目标函数签名以及对应的操作数集合，所述操作数集合包含对应于至少两种预设密文类型的密文操作数；

10 确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中；

在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

2、根据权利要求1所述的方法，其特征在于，还包括：
15 当存在多种预设密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中时，所述目标密文类型为其中层级最低的预设密文类型。

3、根据权利要求1所述的方法，其特征在于，所述将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算，包括：

20 将所述对应于至少两种预设密文类型的密文操作数以及对应于字面量类型的密文操作数解密后分别转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

4、根据权利要求1所述的方法，其特征在于，所述多种预设密文类型属于基于格的偏序集中的元素，所述确定所述至少两种预设密文类型对应的目标密文类型，包含：

25 确定所述操作数集合中的密文操作数对应的所述至少两种预设密文类型在所述偏序集中对应的上确界，以作为所述目标密文类型。

5、根据权利要求4所述的方法，其特征在于，所述偏序集基于拓扑序列进行表征，所述拓扑序列中各元素的边对应于所述单向密文转换关系，且每一单向密文转换关系中的原始密文类型在所述拓扑序列中对应的序号小于对应的目的密文类型在所述拓扑序列中
30 对应的序号，所述确定所述至少两种预设密文类型对应的目标密文类型，包括：

比较所述至少两种预设密文类型中N种预设密文类型在所述拓扑序列中对应的序号大小，当所述N种预设密文类型对应的序号不完全一致时，将所述N种预设密文类型中对应非最大序号的预设密文类型分别更新为与之在所述拓扑序列中的边所对应的预设密文类型，直至所述N种预设密文类型对应的序号一致，所述N为所述至少两种预设密文类型中
35 预设密文类型的种类数目；

将所述拓扑序列中与所述N种预设密文类型的序号对应的预设密文类型确定为目标密文类型。

6、根据权利要求1所述的方法，其特征在于，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，包括：

5 在第一预设密文类型与第二预设密文类型之间相互存在所述单向密文转换关系的情况下，所述多种预设密文类型中包含与所述第一预设密文类型具有相同密文类型的虚拟密文类型，且由所述第二预设密文类型指向所述第一预设密文类型的单向密文转换关系被替换为由所述第二预设密文类型指向所述虚拟密文类型。

7、根据权利要求1所述的方法，其特征在于，还包括：

10 在所述目标密文类型不支持所述目标函数签名对应的函数的情况下，在所述目标密文类型与所述最高层级的预设密文类型之间形成的路径中选取其他预设密文类型以更新所述目标密文类型，所述其他预设密文类型支持所述目标函数签名对应的函数。

8、根据权利要求1所述的方法，其特征在于，还包括：

15 根据接收到的调整指令，调整所述多种预设密文类型所含的预设密文类型和/或所述多层级密文转换关系中的任一单向密文转换关系。

9、一种密文混合运算装置，其特征在于，用于对多种预设密文类型的密文进行混合运算，所述多种预设密文类型之间设有由原始密文类型指向目的密文类型的单向密文转换关系，并基于所述单向密文转换关系形成多层级密文转换关系，每一预设密文类型在所述多层级密文转换关系中对应有唯一的层级，且每一预设密文类型与最高层级的预设密文类型之间至少存在一条由所述单向密文转换关系构成的路径，所述装置包括：

数据接收单元，用于接收目标函数签名以及对应的操作数集合，所述操作数集合包含对应于至少两种预设密文类型的密文操作数；

25 目标密文类型确定单元，用于确定所述至少两种预设密文类型对应的目标密文类型，所述目标密文类型同时处于所述至少两种预设密文类型分别与所述最高层级的预设密文类型之间形成的路径中；

数据运算单元，用于在所述目标密文类型支持所述目标函数签名所指定的运算函数的情况下，将所述操作数集合中所有密文操作数解密后转换为采用所述目标密文类型进行表征，并根据所述目标函数签名所指定的运算函数对转换后的密文操作数进行运算。

30 10、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1~8任一所述方法的步骤。

11、一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1~8任一所述方法的步骤。